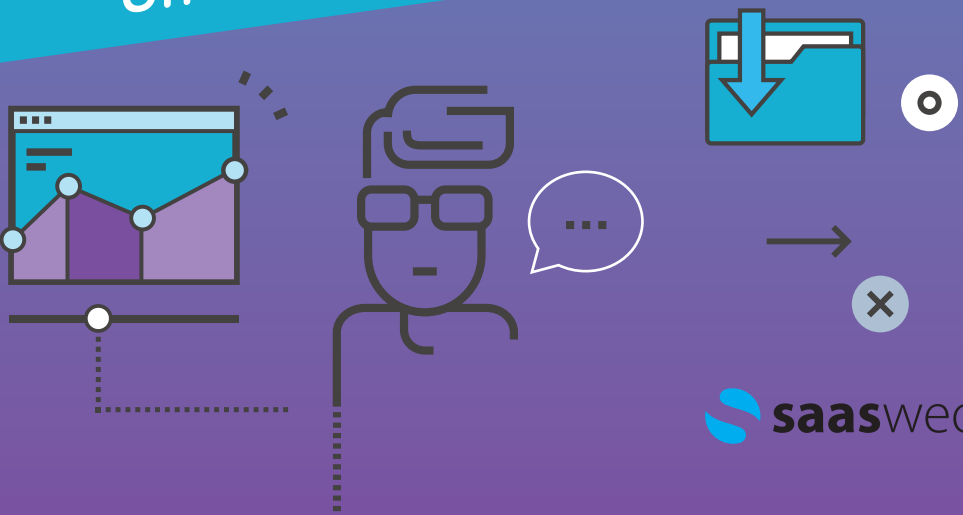
GUIDE PRATIQUE SAASWEDO

LE RGPD ET VOS COLLABORATEURS

Un défi RH et business



saaswedo


Login
Password
Access

AVANT-PROPOS

Le règlement général sur la protection des données à caractère personnel nous concerne tous.
Au-delà de son aspect purement juridique et légal, il constitue surtout une nouvelle vision du monde numérique poussée par les pays européens face aux autres modèles, notamment américain ou chinois. Cette vision de notre économie et de nos usages personnels et professionnels, reconnait ainsi la place centrale de la donnée - et de sa protection - dans tous les équilibres importants pour nos entreprises et nos droits en tant que citoyens. Mais au-delà de cette intention louable, le diable se cache comme souvent dans les détails. Appliqué de façon non-différenciée et impersonnelle, ce règlement, qui a déjà fait couler beaucoup d'encre, pourrait bien briser l'élan formidable de la transformation que de nombreuses organisations réalisent grâce au numérique et à la donnée justement. Cela explique que tant d'entreprises se soient inquiétées des impacts négatifs que pourraient avoir les nouvelles règles sur leur business. L'ambition est donc bien de transformer une apparente contrainte en opportunité. Or, pour y parvenir, de plus en plus d'organisations s'aperçoivent qu'elles dépendent de la capacité de leurs collaborateurs à s'emparer du RGPD dans leur quotidien : pour en faire un argument de marque, pour en faire un facteur de confiance ou encore pour prolonger les valeurs de l'entreprise. La perception qu'ont les collaborateurs du RGPD et la façon dont l'entreprise communique auprès d'eux est donc un facteur clé de réussite.
Nous partageons, avec vous, dans ce carnet les résultats de notre enquête « Le RGPD et vos collaborateurs » réalisée début 2018. Ainsi que les témoignages de directeurs des systèmes d'information, responsables de la sécurité de l'information et gestionnaires de risques, qui ont mis en place des dispositifs spécifiques pour intégrer leurs collaborateurs dans des réflexions structurantes sur le RGPD.

Nous vous en souhaitons une agréable lecture.

Gilles Mezari
CEO de Saaswedo et Administrateur du Syntec Numérique

RGPD, impliquer pour mieux transformer

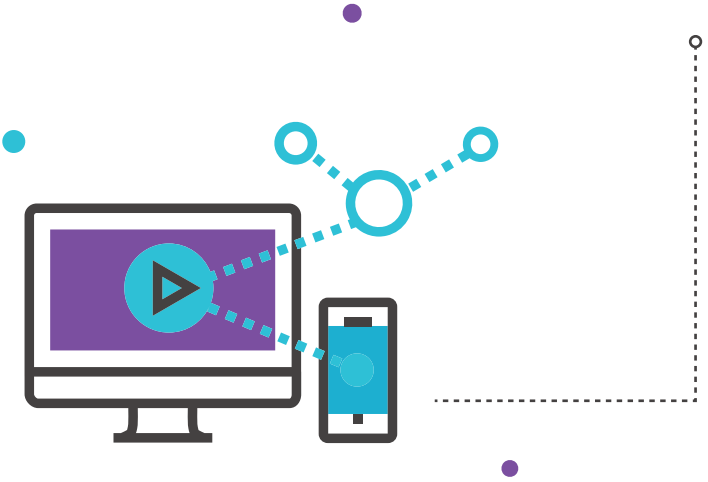
Pendant les derniers mois avant le 25 mai 2018, les entreprises de tout secteur et de toutes tailles ont sonné le branle-bas de combat. La médiatisation croissante autour du règlement général européen sur la protection des données personnelles (RGPD) a en effet considérablement accéléré la mise en place de dispositifs adaptés : nouveaux processus métiers comme modification des systèmes d'information.

Paradoxe : les entreprises entendent depuis longtemps des affirmations contradictoires sur la difficulté de la mise en conformité. Si l'on perçoit le RGPD comme l'évolution naturelle de quarante années de Loi Informatique et Libertés, les surprises sur ses dispositions sont minimales. Si l'on découvre l'enjeu de protection et de confidentialité des données, mis au goût du jour par la croissance exponentielle et peu maîtrisée des usages digitaux de ses clients et collaborateurs, alors le champ d'application paraît au contraire tellement vaste qu'il en devient désespérant. Bien entendu, la réalité pour les entreprises se situe souvent, selon leurs activités, leur culture et leurs projets passés, entre ces deux extrêmes.

Sur l'ensemble des communications concernant le RGPD, on ne peut cependant ignorer un point commun : le fait que les impacts soient avant tout appréhendés par les entreprises sous l'angle de la gestion des données de leurs clients. Or, s'il y a bien un aspect de la transformation actuelle des organisations que l'on ne peut ignorer, c'est le fait que le numérique avec les nouveaux modes de travail qu'il rend possible, contribue largement à rendre floue la frontière entre la vie privée et la vie professionnelle, entre le consommateur et le collaborateur. Malgré cela, le RGPD est encore trop peu abordé dans sa dimension RH. Même les principaux concernés, les collaborateurs, n'imaginent pas toujours que le règlement couvre de facto l'usage que fait leur entreprise de leurs données.

Des impacts sur toutes les autres problématiques du RGPD

Toute entreprise ayant des employés dans l'Union Européenne doit prendre en compte cette réalité, même si son siège n'est, lui, pas dans l'UE. Les droits et devoirs des employés doivent être passés au crible de la grille de lecture RGPD, mais ce n'est pas tout. S'assurer de la bonne compréhension par chacun du sens et de la philosophie du RGPD, est bénéfique pour que les collaborateurs s'engagent sur les autres



sujets sur lesquels le règlement a un impact très fort : la relation client, mais aussi la définition des responsabilités partagées avec les prestataires, sous-traitants, ou encore l'innovation, qui doit dorénavant intégrer la confidentialité et la sécurité « by design ». L'engagement des collaborateurs, la clarification des responsabilités de l'entreprise et de ses salariés, sont autant de clés pour faire de la contrainte réglementaire un levier de valeur. Sans s'intéresser à l'impact RH, beaucoup d'entreprises restent hémiplégiques dans leur vision du RGPD !
C'est ce constat qui a poussé Saaswedo, éditeur français spécialiste des usages télécoms des entreprises, à interroger avec Alliancy, média d'influence sur la transformation numérique, les entreprises sur leurs perceptions du sujet et les actions qu'elles mènent vis-à-vis de leurs collaborateurs. Les résultats de cette enquête sont présentés dans ce recueil (p.12-13). Au-delà des données quantitatives ainsi obtenues, plusieurs sociétés ont accepté de préciser leurs réponses lors d'entretiens individualisés. En effet, la variété des situations et des fonctionnements des organisations rend important d'amener un peu de granularité dans ces traitements du rapport entre le RGPD et les collaborateurs. L'objet des entretiens a notamment été de voir à quel point la perception et les interactions des équipes techniques (SI, digital…) étaient différentes de celles des autres collaborateurs. Et comment avait été gérée la communication vis-à-vis d'eux, voire le cas échéant leur formation. Autre point d'intérêt relevé par Saaswedo, du fait de son expertise dans le domaine des usages télécoms, le RGPD change-t-il la façon dont les organisations appréhendent leur politique de bring your own device ou le monitoring des flux de données issus des terminaux utilisés à des fins professionnelles ?

Les DSI, RSSI, risk managers qui témoignent dans ce recueil ont accepté de nous éclairer sur leurs priorités et les écueils qu'ils ont dû dépasser, face à ces questions. Tous ont en commun d'avoir voulu faire de la mise en conformité obligatoire du RGPD, un atout pour l'avenir de leur organisation. Et tous reconnaissent qu'ils ne sont qu'au début d'un chemin pour lequel il n'y a pas véritablement de ligne d'arrivée. Nul doute que leurs expériences peuvent encore aujourd'hui être des sources d'inspiration précieuses pour d'autres.

« Les questions soulevées par le RGPD permettent à une entreprise de préparer son avenir dans l'économie numérique »

Jérôme Siméon,
Président de la commission juridique du Syntec Numérique

Jérôme Siméon, président de la commission juridique du Syntec Numérique explique la perception qu'ont les adhérents du syndicat sur le RGPD. Et il alerte : les entreprises qui veulent demain profiter de la valeur de leur transformation numérique, doivent apprendre à mieux maîtriser leurs rapports aux données.

Au sein du Syntec Numérique, dans quel cadre se sont effectués les travaux concernant le RGPD ?

En 2017, le conseil d'administration du Syntec Numérique a lancé un grand thème de travail sur le sujet de la donnée et de la nouvelle place que celle-ci prenait dans la stratégie et la transformation des entreprises. Cela a notamment abouti à la tenue du Grand Débat sur la donnée au printemps 2018 et à l'émergence d'outils pratiques pour nos adhérents. Une part de ces outils (fiches pratiques, référencements de prestations, conférences…) concernait directement le RGPD. Car si les grands groupes se sont mobilisés sur le sujet depuis longtemps, nous comptons également beaucoup d'ETI, de PME et de start-up parmi nos membres. Ces entreprises avaient besoin d'être sensibilisées, puis accompagnées dans la mise en application du règlement. Nous avons, par exemple, mis en place une ligne téléphonique dédiée à l'accompagnement juridique de nos membres. Et le RGPD a été – tout sujet confondu – le thème sur lequel nous avons été le plus sollicité et questionné.

Quelle est la perception de vos adhérents sur le règlement ?

Une des questions que se posent beaucoup d'entreprises est de savoir si le RGPD va être un frein majeur à leur business. Finalement, il n'y a pas de certitudes, cela dépendra à quel point les règles sont appliquées intelligemment ou brutalement. Mais ce qui est certain, c'est que la mise en conformité passe de toute façon par un inventaire de son patrimoine informationnel. Or, quand on se transforme avec le digital, force est de reconnaître qu'un tel inventaire a énormément de valeur. De fait, avant le RGPD, celui-ci a rarement été mené par les entreprises. Par ailleurs, cet inventaire va avoir un impact positif sur la sécurité des entreprises. Dans le contexte actuel de croissance des menaces cyber, la valeur est là aussi claire.

Enfin, gardons à l'esprit que la donnée est tout simplement la matière première des démarches d'innovation. Que ce soit pour créer de nouveaux services avec l'intelligence artificielle ou pour améliorer sa plateforme d'e-commerce, le lien entre la maîtrise de ses données et l'impact business final est très fort. Le RGPD est l'occasion d'améliorer cette maîtrise.

Cette opportunité repose sur un bon équilibre à trouver dans l'application du RGPD. A quel point est-il difficile à atteindre ?

La condition principale pour trouver cet équilibre est que chacun, dans la chaîne de valeur économique, doit prendre sa responsabilité pour permettre une amélioration globale. L'une des grandes nouveautés du RGPD réside ainsi dans le principe d'« accountability », qui doit permettre d'éviter aux organisations – qu'elles soient responsables de traitement (RT) ou sous-traitantes (ST) – de se décharger sur d'autres de leurs obligations. Sans cela, il y a en effet le danger qu'un déséquilibre préjudiciable s'installe dans la relation contractuelle avec les sous-traitants. Chacun dans la chaine essayant d'en faire le moins possible. Ces visions court-termistes occultent les dégâts que l'on va causer plus tard à la fois à nos relations BtoB et à la confiance des clients finaux. De plus, beaucoup d'acteurs se retrouvent à la fois à être RT et ST. C'est l'occasion d'essayer de comprendre ce qu'impliquent ces différentes responsabilités plutôt que de devenir schizophrène…

Les autorités sont-elles suffisamment sensibles à cette question ?

Le dialogue avec les autorités compétentes et notamment le G29 – avec particulièrement en France la Cnil – est le deuxième levier d'action du Syntec Numérique, au côté de l'aide apportée aux adhérents. Il faut reconnaître que très tôt le régulateur a fait preuve d'ouverture et a envoyé de nombreux signaux positifs, notamment vis-à-vis des PME. Sur la question précise du partage de responsabilité entre RT et ST, la Cnil estime ne pas avoir à s'immiscer dans les relations contractuelles des entreprises. Elle ne crée donc pas de déséquilibre, mais il nous paraît nécessaire qu'elle envoie quelques messages forts pour pousser certains à se remettre en question. La Cnil doit profiter de son excellente réputation pour ne pas être seulement un organe de coercition, mais pour éviter que l'esprit du RGPD soit dénaturé à l'usage.

Quel message vous paraît-il important de faire passer aux entreprises aujourd'hui ?

Il faut préparer la suite dès maintenant et ne pas voir la date de mise en application du RGPD comme une finalité. Il faut également mettre en œuvre ses responsabilités et ne pas vouloir à tout prix s'en défausser sur d'autres. Ces deux points sont ce qui permet de faire de la contrainte une opportunité. Si vous voulez capitaliser demain sur l'IA par exemple, vous ne pouvez pas ignorer ces sujets. En effet, en vous défaussant sur vos sous-traitants, vous leur confiez sans le vouloir la maîtrise de la réflexion sur votre avenir. En voulant régler un problème de risque juridique, un responsable de traitement peut s'aliéner en fait la visibilité et la maîtrise des sujets fondamentaux du numérique indispensables pour ses activités de demain, qui vont toutes s'appuyer sur la data.

A qui doit s'adresser cette alerte au sein de l'entreprise ?

Aux dirigeants bien sûr, mais pour faire naître cette conviction à tous les niveaux de l'entreprise, il va falloir accompagner les collaborateurs et communiquer intelligemment auprès d'eux. La mobilisation des juristes, des DSI et des dirigeants, seule, ne suffit pas. Un exemple : si un salarié souhaite exercer son droit à l'oubli, l'entreprise a un mois pour réagir. C'est extrêmement court : cela veut dire que vos collaborateurs du service RH doivent bien connaître le sujet, ce qu'il y a à faire opérationnellement mais aussi le sens que l'on donne à cette demande. Comment espérer sinon qu'ils priorisent efficacement ? La sensibilisation au RGPD permet de créer des synergies autour des réalités de notre économie numérique, de générer de la transversalité et de la confiance… Bref, de faire bien plus que seulement appliquer une contrainte.

" IL FAUT PRÉPARER LA SUITE DÈS MAINTENANT ET NE PAS VOIR LA DATE DE MISE EN APPLICATION DU RGPD COMME UNE FINALITÉ. "

Syntec NUMÉRIQUE

« Quand on évoque la donnée personnelle, nos collaborateurs pensent avant tout aux impacts business ! »

Laurianne Thiebaut,
DSI d'Essilor France

Laurianne Thiebaut, DSI d'Essilor France, revient sur les dispositions prises pour accompagner les équipes de développeurs pour apprivoiser le RGPD. Celui-ci étant étant perçu comme une opportunité de marque pour le leader mondial du verre correcteur.

Quelles responsabilités ont échoient à la DSI d'Essilor France dans le cadre de l'entrée en application du RGPD ?
La DSI de la filiale France d'Essilor est une DSI de proximité, résolument axée métier, notamment à travers le développement d'applicatifs innovants. C'est la DSI Groupe qui s'occupe des infrastructures au niveau monde, et par extension des enjeux de sécurité. Or, le grand changement entraîné par le RGPD est qu'il amène à prendre bien différemment en compte la sécurité, avec un focus nouveau sur les données et les applicatifs. Les DSI des filiales, comme nous, doivent donc également monter au créneau.

Comment vous êtes-vous coordonnés ?
Le groupe a recruté début 2017 un data protection officer, au sein du département juridique, pour se concentrer à plein temps sur les problématiques transversales impliquées par le RGPD. C'est donc lui qui est devenu notre premier point de contact et qui a orchestré la diffusion des informations de manière cohérente. Depuis un an, il ne passe pas une semaine sans que nous échangions directement, dans un objectif de coordination et de co-création.

C'est-à-dire ?
Nous avons vu le RGPD comme une opportunité, notamment pour asseoir la réputation de sérieux d'Essilor vis-à-vis du marché et de nos clients. En tant que leader mondial du verre correcteur, il est apparu comme une évidence que nous devions nous organiser de façon à apporter un vrai sens métier et technique à une telle contrainte réglementaire. Pour y arriver, le marketing a été intégré très tôt dans les discussions. En la matière, cela a été un vrai avantage d'avoir un DPO qui ne soit pas un acteur technique. Sans cette casquette, il a pu faire passer des messages clés et dès le départ, nous avons ainsi pu éviter de tomber dans le piège du « sujet data qui ne concerne que les informaticiens ». Cela a permis d'intégrer beaucoup plus intuitivement cette attention portée à la donnée directement au sein des processus métiers.

Qu'en est-il de la dimension purement technique pour la DSI ?
Le plus grand défi est, en fait, de mettre en œuvre techniquement une dimension légale, même une fois que l'on est d'accord sur les processus. Au-delà de la question du registre des traitements de données, la difficulté réside dans la partie concernant la cybersécurité

et la traduction concrète et opérationnelle du concept de « privacy by design ». Nous avons un plan d'action pour faire évoluer progressivement notre legacy... mais sur quels piliers devons-nous nous appuyer pour les nouveaux développements qui sont au cœur de l'activité de la DSI France ? Certains standards de sécurité historiques ont été démocratisés par le RGPD, mais il nous manque vraiment des détails - sur les API authentifiés, sur les procédures et périmètres de chiffrement/déchiffrement... - pour remplir la « boîte à outils » dans laquelle tous nos développeurs vont devoir piocher.

Comment ces derniers perçoivent-ils le changement ?

Nous travaillons avec beaucoup d'équipes externes et de freelances. Contrairement à ce que l'on pourrait croire, ils ont une vraie appétence pour les questions de sécurité, qui est vue comme partie intégrante de ce qu'ils doivent livrer à un client. Mais le RGPD va un cran plus loin... voire, quand on commence à se poser des questions, beaucoup plus loin. Nous avions déjà des habitudes et des règles que nous transmettions aux développeurs. Mais pour que tous les réflexes attendus par le RGPD se diffusent chez tous les développeurs, de façon cohérente et harmonieuse pour tous nos projets, il va falloir être encore plus méticuleux. Cela est passé par une formation des chefs de projet fin 2017, suivie d'une formation pour toutes les équipes IT au début de l'année, puis une nouvelle fois en avril. Nous avons ensuite mené un brainstorming avec eux pour mettre le doigt sur les manques, les interrogations et les besoins concernant le « package de base » auquel devait accéder tout développeur. Avec un prestataire externe, nous avons également travaillé sur les méthodes qui nous permettraient de nous auditer nous-mêmes et de surveiller nos progrès en la matière.

" NOUS TRAVAILLONS AVEC BEAUCOUP D'ÉQUIPES EXTERNES ET DE FREELANCES. CONTRAIREMENT À CE QUE L'ON POURRAIT CROIRE, ILS ONT UNE VRAIE APPÉTENCE POUR LES QUESTIONS DE SÉCURITÉ "

Avez-vous un exemple de projet impacté par la mise en œuvre de votre réflexion ?

Le cas le plus évident est celui des évolutions menées sur nos sites web. La partie visible de l'iceberg était de revoir notre gestion de l'opt-in et du consentement pour nos clients, et par extension de la suppression des données, si besoin. La partie immergée à laquelle nous avons maintenant envie de nous attaquer est d'aller jusqu'à revoir notre modèle d'architecture. Notamment autour des données plus sensibles pour en garantir la protection tout au long de leur cycle de vie, grâce à des services d'encodage et de décodage et de déchiffrement... Le RGPD nous a fait porter un regard complètement nouveau sur ces aspects, même si cela implique de fondamentalement changer notre philosophie en matière d'infrastructure IT.

Vos collaborateurs se sentent-ils eux-mêmes directement concernés par les dispositions du règlement ?

Quand on évoque la donnée personnelle, ils pensent avant tout aux impacts business ! En ce sens le RGPD n'est pas perçu comme un sujet RH. Pourtant, il y a effectivement des points d'attention à avoir en la matière. Nos forces de vente utilisent par exemple des tablettes fournies en France par la DSI, mais de facto rien n'est bridé sur ce matériel et les usages personnels sont tolérés. Nous allons devoir clarifier les règles de façon constructive, car il est très important que chaque collaborateur s'approprie le sujet. Le champ couvert par le règlement est très large : si une entreprise ne veut pas se retrouver à courir en permanence derrière la problématique des données personnelles, il faut éviter de se dire que c'est l'informatique qui va toujours déterminer ou interdire les usages dans le détail. Chacun va devoir se prendre en main, que ce soit dans son rapport avec les clients, ou quand il échange un document en interne avec des collègues.

ESSILOR
MIEUX VOIR LE MONDE

Enquête : Le RGPD et vos collaborateurs

Quatre-vingt-dix entreprises ont accepté de répondre à l'enquête menée par Saaswedo en partenariat avec la rédaction d'Alliancy.

Les DSI, RSSI, risk managers… étaient invités à s'exprimer durant le mois de février 2018 sur différents points : leur perception du niveau de contrainte représenté par le RGPD, sur les actions menées auprès des collaborateurs – dans les équipes techniques et métiers – et sur les services internes et organisations externes qui ont été associés en priorité au projet de mise en conformité. Les résultats font apparaître une prise de conscience récente, un bon espoir de dépasser les difficultés du RGPD pour générer de la valeur, et une différence.

Une difficulté réelle *mais des opportunités business*

51,7%
Le RGPD est complexe mais peut être mis en œuvre efficacement

28,1%
Le RGPD est beaucoup trop complexe

Seules
11%
des entreprises se sont déclarées prêtes pour le **25 mai 2018**

Mais
62,9%
voient dans le règlement « une opportunité pour le business »

« La transparence et le "cercle de confiance" institués avec l'usager sont primordiaux »
« C'est l'occasion d'une démarche de réorganisation et de refonte de nos procédures »
« C'est un élément de différenciation par rapport aux concurrents »
« De vraies possibilités de communication en interne et à l'externe »

Les collaborateurs : *une grande inconnue à résoudre en priorité*

45%

des organisations ne savent tout simplement pas quelle perception leurs collaborateurs ont du RGPD

89%

des entreprises ont prévu des opérations de communication en interne vis-à-vis du RGPD

Mais seulement **1 sur 2**

a mis en place des moyens pour gérer ses obligations vis-à-vis de ses propres collaborateurs

« Nous avons organisé des ateliers avec certaines personnes dans le cadre d'un audit mais ce n'est pas suffisant. »
« Plus que des formations... un sujet d'acculturation à la donnée »
« Il a fallu interviewer les directions métiers »
« Il est important de différencier les formations RGPD pour les collaborateurs et la formation technique pour les équipes IT »

Des travaux menés récemment *et avant tout en interne*

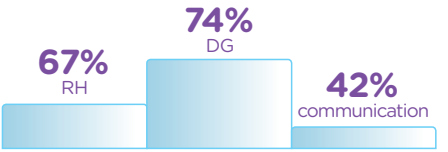
Seules

18%

des entreprises ont mis en place un groupe de travail avant 2017

42% depuis 2017

Les RH sur la 2e marche du podium des participants internes, preuve de la préoccupation vis-à-vis de l'impact sur les collaborateurs



Les entreprises limitent les interventions extérieures pour gérer le RGPD.

Seules

46% des entreprises ont fait appel à un **cabinet d'avocats**

20% à un **cabinet de conseil IT**

14% à un **cabinet de conseil en stratégie**

Les témoignages sont issus de l'enquête menée par Alliancy.

« La vision RGPD de l'entreprise doit s'appuyer sur des valeurs auxquelles les collaborateurs adhèrent déjà pour qu'ils perçoivent une continuité »

Winoc Coppens,
DSI de 20 Minutes

×

Winoc Coppens, DSI du quotidien français 20 Minutes, explique comment il a mené la sensibilisation, de collaborateurs variés, au RGPD et l'impact de la mise en conformité sur la stratégie d'innovation du média.

Dans votre réflexion sur le RGPD, la date du 25 mai 2018 a-t-elle été une borne importante ?
Le RGPD est complexe à prendre en compte pour une entreprise car c'est un sujet très vaste. Même ceux qui, comme nous, se sont lancés il y a quelques temps, continuent d'intégrer de nouvelles personnes et de nouveaux sujets dans la réflexion. Le discours parfois entendu, qui implique d'être prêt au 25 mai, n'a jamais été le plus important. Le RPGD est avant tout un sujet d'amélioration continue. Dans cette optique, la DSI de 20 Minutes a isolé un budget spécifique pour traiter ce caractère structurant. Cela nous a notamment permis de nous équiper d'un outil pour mieux informer nos lecteurs et maîtriser les cookies sur notre site web. En la matière, le RGPD est surtout une opportunité pour nous aider à prioriser les sujets sur le long terme et à renforcer la sécurité.

Qui porte le projet ?
Je suis missionné en binôme avec le responsable du développement numérique de 20 Minutes pour initier et accompagner ces changements. Nous n'avons pas vocation à garder ce rôle de Data Protection Officer, car nous ne pouvons pas être à la fois juge et partie. Le DPO sera donc externalisé, ce qui nous permet de disposer d'une compétence juridique et d'une prise de recul sur nos actions avant validation. Nous sommes également les référents et garants dans l'entreprise pour accompagner au quotidien les responsables de traitement des différents services sur ce règlement. Nous souhaitons parvenir à insuffler une approche de "Privacy by design".
Nous sommes également accompagnés par une agence spécialisée – Alter Privacy – qui nous apporte les soutiens nécessaires.

Comment avez-vous procédé ?
Pour mieux sensibiliser les collaborateurs, nous nous sommes avant tout basés sur les conseils de la Cnil. Notamment à travers les 6 étapes de mise en conformité. La première d'entre elle concerne la nomination d'un DPO, ou de deux dans notre cas. Cela a permis d'articuler une communication auprès de toute l'entreprise, venant du président lui-même. Nous avons ensuite mené des réunions avec les référents qui ont été nommés dans chaque service, afin de préparer l'animation des ateliers de sensibilisation sur le RGPD. Mais également pour faciliter la première version de la

cartographie des traitements des données à caractère personnel. Nous avons pris le parti de faire fortement confiance à ces référents pour communiquer auprès des autres collaborateurs. Nous menons également un sondage mensuel auprès de toute l'entreprise qui permet de mesurer, en moins de 5 minutes, l'implication récurrente vis-à-vis du RGPD sur les projets menés par les collaborateurs. Cela est conduit en parallèle d'ateliers gérés avec des avocats, pour aller plus loin, cette fois-ci sur la base du volontariat.

Quelles ont été les réactions des collaborateurs ?

Quand on explique le principe du RGPD, c'est un changement en général bien compris, d'autant que les collaborateurs sont également concernés à titre privé. Mais ce sont les effets en termes de charge de travail supplémentaire et les changements qu'ils induisent qu'il faut gérer, car ils peuvent être stressants pour les collaborateurs. La tentation est grande de systématiquement reporter à plus tard les évolutions des pratiques au quotidien. On gagne en efficacité globale quand tout le monde y consacre juste un peu de temps en plus. Et pour y arriver, il faut générer un véritable engagement. Il faut donc avoir, du côté de l'entreprise, une vision claire qui reprenne des valeurs auxquelles les collaborateurs adhèrent déjà pour qu'ils voient ces évolutions comme une continuité logique. Dans notre cas, il s'agit du contrat de confiance que nous avons vis-à-vis de nos lecteurs et qui fait que nous avons un modèle économique qui nous permet de ne jamais avoir eu à céder de données personnelles.

" LE RGPD EST UNE OPPORTUNITÉ POUR NOUS AIDER À PRIORISER LES SUJETS SUR LE LONG TERME ET À RENFORCER LA SÉCURITÉ. "

Tous les services de votre organisation se posent-ils la question de la même façon ?

Un des enjeux est que nous avons une population de collaborateurs variée, avec des « usages numériques » différents. Par exemple : nos commerciaux sont équipés de smartphones fournis par l'entreprise, là où le bring your own device est pratiqué pour nos journalistes. Ce sont eux qui viennent nous demander de les connecter à une application ou aux e-mails. Cela nécessite que nous développions une vigilance spécifique sur le consentement. A l'ère du RGPD, il nous faut encore plus clarifier les responsabilités de l'entreprise et des collaborateurs face aux usages en mobilité, aux accès e-mails à distance…

De manière générale, quels sont les points qui vous ont le plus aidés à avancer vers votre mise en conformité ?

Une bonne cartographie des traitements et données, une approche en mode projet et une capacité de la DSI à fédérer autour d'elle grâce à une vision transversale, ont été de vrais accélérateurs. C'est pour cela que la priorité dans une organisation est vraiment de réaliser cette cartographie et de mener les actions de sensibilisation et de communication auprès des utilisateurs.

Quel est le poids du RGPD sur votre stratégie d'innovation ?

Nous avons beaucoup de démarches d'innovation qui sont nées ces derniers mois en parallèle de notre mise en conformité. Ce n'est pas rédhibitoire, même si cela demande une certaine vigilance. En fait, il faut pouvoir faire des nouveaux projets des catalyseurs pour améliorer la maîtrise de nos données. Nous n'avions, par exemple, pas de CRM car le modèle de 20 Minutes n'est pas basé sur l'abonnement. Le fait de mener ce travail de centralisation de la donnée, va nous permettre de gérer le consentement et de nous assurer du sens que l'on donne à ces données. De la même manière, tout ce que nous sommes en train de mener en matière d'intégration de l'intelligence artificielle dans nos services, par exemple avec les chatbots, est l'occasion de challenger nos partenaires et de nous assurer qu'ils prennent le RGPD autant au sérieux que nous. En la matière, ce n'est donc pas un frein, mais un levier intéressant pour amener des changements cohérents dans l'ensemble de nos nouveaux projets.

20 minutes

« En abordant la question de la protection des données personnelles des citoyens, nous avons vu un effet miroir pour les données RH »

Sylvain Bonenfant,
Risk manager
du département
de Seine-Maritime

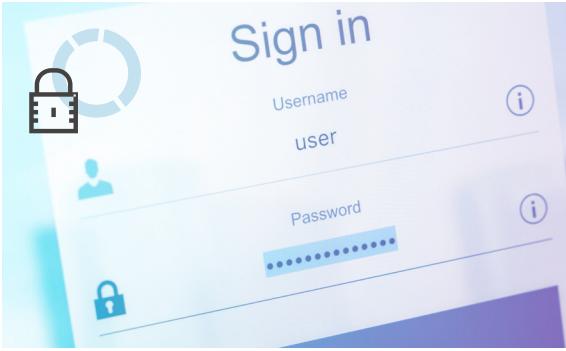
Le département de Seine-Maritime s'est mobilisé sur la protection des données personnelles depuis plus d'une décennie, ce qui lui a permis d'anticiper l'entrée en vigueur du RGPD. Sylvain Bonenfant, son risk manager détaille le cheminement effectué et l'impact pour les agents.

Quel est votre avis sur la très forte médiatisation autour du RGPD ces derniers mois ?
Nous sommes restés sereins car contrairement à ce que l'on a pu entendre, le RGPD ne révolutionne pas la loi informatique et libertés de 1978. Pour les organisations qui suivaient celle-ci, il n'est donc pas un défi insurmontable. Dans notre cas, par exemple, nous avons désigné un correspondant informatique et liberté (CIL) en 2008. Puis en 2010, nous avons commencé à mettre au point une méthodologie de mise en conformité, qui s'est avérée parfaitement compatible avec ce qui était attendu par le RGPD. Les organisations qui n'ont pas anticipé se retrouvent en difficulté, car tout cela prend du temps. Si on regarde par exemple la nomination obligatoire d'un DPO avec le RGPD, on peut se demander où vont le trouver ceux qui n'ont pas réfléchi à la question avant 2018 : les bonnes compétences sont rares ! La formation et la montée en compétence des personnes désignées va prendre du temps !

A quel point le RGPD implique-t-il un changement de culture dans votre organisation ?
Tout le monde est concerné : le président du conseil départemental au même titre que les agents en poste dans un centre médico-social. Les données à caractère personnel sont en effet le carburant de toutes les actions des acteurs territoriaux. Il faut donc absolument sensibiliser et éduquer sur la question de leur protection et de leur confidentialité, et ce, le plus possible individuellement – afin que personne ne soit tenté de penser que c'est surtout le travail des autres et des experts. Tout l'enjeu du RGPD pour les organisations est bien de développer une culture de la protection des données, dont tout le monde va être un acteur.

Quelles ont été vos actions principales pour communiquer auprès des agents en ce sens ?
Nous avons commencé par définir un réseau de contacts dans les services, des ambassadeurs qui ont été formés en un ou deux jours pour permettre à ces nouveaux usages de mieux prendre pied partout. En complément, nous avons sensibilisé rapidement l'ensemble des agents, avec un atelier de deux heures et des séances de questions-réponses pour répondre à leurs inter-

rogations. Nous avons également fait un usage important du journal interne, afin d'informer sur les grandes dispositions adoptées par le département, comme la nomination du CIL, puis du DPO, la nature des sanctions et les analyses d'impacts réalisées. Notre avantage est que nous avions déjà les processus en place pour permettre cela. Au total, cette adaptation et la sensibilisation qui a été réalisée à l'échelle du département nous ont pris environ deux ans. Imaginez l'investissement que cela représente pour ceux qui ont découvert le sujet récemment et doivent suivre le même chemin !



Avez-vous commencé le travail par certains types de données en particulier ?

Nous avons commencé naturellement par nous poser la question de la protection des données personnelles des usages, et notamment celle de notre structure la plus importante, la solidarité, qui représente la moitié du budget annuel du département. Mais dès que nous avons avancé dans ces travaux, il y a eu un effet miroir, avec des questionnements de plus en plus importants des agents eux-mêmes sur ce que représentaient ces questions pour d'autres types de données et d'acteurs. Une dimension RH s'est donc rapidement dégagée de nos premières initiatives. Ce sont des effets en cascade qu'il a fallu traiter. De la même façon, la DSI, qui gère les applications de traitement de données, a dû passer d'une logique où chaque traitement était pris en compte par une application indépendante, à une approche plus intégrée, qui les inclut dans une chaine plus réaliste où elles ont

" L'ENJEU DU RGPD EST DE DÉVELOPPER UNE CULTURE DE LA PROTECTION DES DONNÉES, DONT TOUT LE MONDE VA ÊTRE UN ACTEUR. "

une influence les unes sur les autres. Le traitement des données personnelles ne survient jamais en vase clos, il faut donc mesurer les effets de bord, qu'ils soient techniques ou d'usages pour que l'on s'assure de bien couvrir la réalité et la finalité d'un traitement.

Pouvez-vous donner un exemple de ces « effets de bord » ?

Un agent public est soumis au secret professionnel dans ses activités, mais c'est aussi un citoyen comme les autres. Il utilise son smartphone et les réseaux sociaux au quotidien, et il faut donc qu'il maîtrise la nature des informations auxquelles il accède et qu'il peut diffuser – consciemment ou non. L'exemple type est celui de la messagerie à laquelle on accède en mode web, par exemple depuis son smartphone. Il faut absolument pouvoir rendre les agents acteurs de la protection de l'information à ce niveau.

Dans ce cadre, la collectivité fournit des terminaux mobiles aux personnels encadrants, mais ne peut le faire pour tous les agents. Nous n'avons cependant pas de véritable politique BYOD pour le moment. Il nous faut donc une vigilance sur le fait que les agents utilisent leurs téléphones pour des usages « normaux ». Nous pensons que la logique culturelle, éducative, avec formation et sensibilisation, est bien plus efficace à termes que d'ajouter encore et encore des contraintes. En la matière, vu l'étendue du périmètre concerné par le RGPD, le DPO a de toute façon vocation à être avant tout un chef d'orchestre plutôt qu'un policier. Et pour emmener tout le monde dans le sillage des bons usages, il faut établir une réciprocité de la part de l'organisation, en clarifiant au mieux les responsabilités et les engagements des uns et des autres, en adoptant une vraie politique de transparence RH.

Seine-Maritime
Le Département

« Il faut faire comprendre aux collaborateurs que le cœur du sujet n'est pas l'informatique »

Julien Bourteele,
DSI adjoint
et RSSI de Stelliant

Julien Bourteele, DSI adjoint et RSSI de Stelliant, groupe français spécialiste des services et de l'expertise à l'assurance, détaille l'accompagnement des collaborateurs de l'entreprise vis-à-vis du RGPD. Un point que l'ETI a estimé prioritaire dans le cadre de sa mise en conformité.

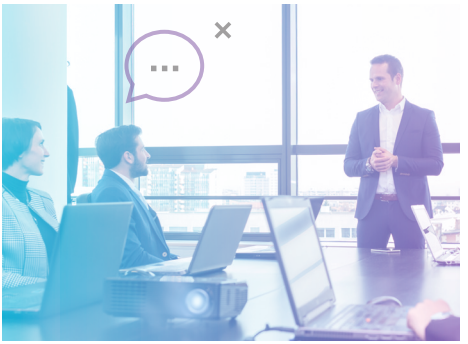
Quel regard portez-vous sur la mise en application du RGPD ?
Vu de la DSI et du RSSI, le RGPD a été un point de départ pour toucher la direction, et remettre à plat des sujets qui avaient eu tendance à rester enfouis depuis longtemps. Nous avons pu nommer une DPO, notre responsable juridique. Nous avions une CIL, en poste dans notre service RH, mais celle-ci va transmettre progressivement ses responsabilités. La DPO a une vraie position de neutralité, vis-à-vis de tous les services, en rapportant directement à la direction générale. En 2017, nous avons travaillé avec elle sur un chantier très important et transversal : le registre des traitements de données. Nous avons mené une revue des spécificités des données personnelles utilisées dans nos différentes activités. En parallèle, nous avons mené une revue vis-à-vis de nos partenaires. D'abord sur les contrats existants, afin de leur ajouter une annexe RGPD permettant de préciser les responsabilités respectives, puis sur tous les nouveaux contrats.

Ces revues étaient vos priorités dans le cadre de la mise en conformité ?
L'esprit de la démarche est celle de l'amélioration continue. Il est donc surtout prioritaire d'avoir en place les processus qui vont permettre de mener ces itérations progressivement et de corriger le tir quand on découvre de nouveaux sujets, en interne ou avec nos partenaires. Pour cela il faut avoir une fondation solide. Pour s'assurer de la pérennité de cette amélioration,

" NOUS AVONS SANCTUARISÉ UN BUDGET RGPD, QUI A ÉTÉ SPONSORISÉ DIRECTEMENT PAR LE PRÉSIDENT DU DIRECTOIRE "

nous avons sanctuarisé un budget RGPD, qui a été sponsorisé directement par le président du directoire. Il n'était pas question d'en faire une partie du budget de la DSI, ce qui aurait eu tendance à le rendre moins transversal.

Qu'est-ce qui vous a permis d'avancer le plus efficacement sur le registre des traitements de données ?
Comme pour la mise en conformité en général,



il n'y a pas de « big bang » mais plutôt une approche incrémentale qui crée de la valeur ajoutée, un pas après l'autre. Cela passe par énormément de communication et de formations vis-à-vis des responsables métiers. Nous avons organisé, avec un consultant externe, des ateliers pour les responsables de traitement, département par département, afin de les sensibiliser sur les fondations du RGPD. Mais aussi pour qu'ils s'engagent dans la co-construction des registres, chacun de leur côté. Nous ne voulions pas assurer à nous seul la définition du contenu du registre, car c'est un sujet éminemment métier.

Concrètement, comment les collaborateurs ont-ils été intégrés à la démarche ?

La pédagogie est clé. En effet, quand on aborde la question du RGPD avec les collaborateurs, on entend rapidement répondre qu'il s'agit d'un sujet informatique. Il faut alors leur faire comprendre que le cœur du sujet est celui des processus : la technique n'est qu'un sous-jacent, qui ne peut pas être le moteur. De plus, notre contexte est particulier car nous sommes dans une énorme période de suractivité, avec près de 30 % d'activité supplémentaire par rapport à la même période l'an passé. Nous avons très vite identifié le risque d'assommer les collaborateurs avec la problématique RGPD, si on ne faisait pas attention. Nous travaillons donc à faire des responsables de traitement, avant tout, des ambassadeurs qui vont pouvoir prêcher la « bonne parole RGPD » dans leurs services respectifs. Pour y parvenir, j'organise des campagnes de sensibilisation comme je peux en faire par exemple sur la sécurité. Ce sont des sujets très sérieux sur lesquels il faut savoir amener un peu de légèreté et parfois d'humour, pour provoquer une prise de conscience sans stigmatiser. En la matière, des outils originaux peuvent être utilisés : des petites bandes dessinées, des partages d'anecdotes en face à face… Je travaille directement avec les équipes marketing du groupe pour trouver le bon moyen d'adresser par petites touches le sujet auprès de tous les collaborateurs, que ce soit en groupe ou par des e-mails ciblés. L'erreur serait de vouloir tout faire, tout de suite, et de complètement diluer les messages.

Est-ce que cela implique également des façons de travailler différentes pour vos équipes ?

Nous avons un vrai questionnement sur les usages de nos collaborateurs. Typiquement, nous utilisons comme beaucoup d'entreprises une messagerie online : Microsoft Office 365. Les collaborateurs peuvent y accéder avec un ordinateur personnel ou leur smartphone. Mon objectif est de profiter du RGPD pour amener un peu de souplesse, tout en clarifiant les responsabilités de l'entreprise et du collaborateur vis-à-vis des données personnelles.
Nos experts « terrain » travaillent eux avec des applications métier, mais cela ne se fait qu'avec des accès VPN et une conteneurisation de la donnée au niveau des datacenters. De plus, nous leur fournissons les terminaux pour accéder à cette application.

Percevez-vous le RGPD comme un frein ou une opportunité, par rapport aux spécificités de votre activité ?

Nous constatons déjà depuis un certain temps, dans le cadre des demandes que l'on reçoit de nos clients, que les principes clés du règlement apparaissent de plus en plus fortement. Ils ne portent pas toujours cette étiquette RGPD, mais ils sont bien là. Nous avons donc eu la chance d'avoir pu anticiper et adresser sérieusement le sujet. Nous commençons ainsi à avoir des retours positifs de nos différents partenaires où l'engagement de nos collaborateurs et la mise en place des bons processus sont remarqués.

stelliant

« Les entreprises passent à côté des impacts du RGPD sur leurs collaborateurs »

Gilles Mezari,
CEO de Saaswedo et Administrateur du Syntec Numérique

Gilles Mezari, CEO de Saaswedo et Adminitrateur du Syntec Numérique explique pourquoi le sujet du rapport des collaborateurs au RGPD mérite de figurer au rang des priorités pour les organisations en 2018.

A quel point les entreprises sont-elles à l'aise avec l'entrée en vigueur du règlement général européen sur la protection des données personnelles (RGPD) ?
Le sujet a été extrêmement médiatisé depuis quelques mois. Rares sont les entreprises à ne pas avoir conscience de ce qui arrive, et heureusement ! Leurs directions juridiques et leurs DSI sont souvent déjà sur le pied de guerre. Mais plus que sur la mise en conformité, on sent cependant une interrogation persister chez les dirigeants d'entreprise : comment faire pour que le RGPD ne soit pas un frein au business ?

Tous les sujets propres au RGPD sont-ils pareillement pris en compte ?
C'est justement le problème : la prise de conscience est assez partielle. L'attention et les mesures les plus médiatiques sont celles portées vis-à-vis des données des clients. Ce cœur de sujet est un gros morceau pour les entreprises, mais du coup, elles passent souvent à côté des impacts du RGPD vis-à-vis de leurs collaborateurs. Autant les conseils et avis d'experts pullulent pour aider les entreprises à améliorer la gestion des informations relatives à leurs clients – et leur consentement dans leur utilisation ; autant tout cela est beaucoup plus flou du point de vue des salariés.

Pourquoi cette différence ?
Comme les clients, les collaborateurs partagent beaucoup de données personnelles avec l'entreprise. Ils peuvent même être amenés à partager des données beaucoup plus confidentielles que leurs nom, adresse… comme leur état de santé par exemple. Or, dans le cas où les données sont « bénignes », la relation collaborateur-entreprise n'est pas vraiment chamboulée par le RGPD. Alors qu'une vigilance toute particulière s'impose pour encadrer la gestion des données plus sensibles. Et encore faut-il arriver à les distinguer. En effet, il n'y a pas de listing précis de ce qu'est une « donnée personnelle » dans ce cadre. Et aujourd'hui, les collaborateurs – tout le monde, peut-on dire – entremêlent constamment des usages professionnels et personnels. Ils le font d'ailleurs à partir des mêmes outils, notamment leur smartphone. La capacité de l'entreprise à comprendre ce qu'il en est, sans être invasive dans le cadre du RGPD, est donc sérieusement interrogée.

Qu'est-ce qui peut changer la donne au sein des entreprises, pour aider à réconcilier les deux mondes ?

Un premier point d'action est d'agir à la source, au niveau de la gestion des télécoms – qui sont au centre des usages data des collaborateurs. Il faut ainsi être capable de déterminer quels sont les usages et les flux de données qui dépendent de la vie personnelle d'un collaborateur, de ceux qu'il utilise pour le travail et qui sont sous la responsabilité de l'entreprise. Cela signifie avoir une gestion des télécoms, par exemple, qui intègre les processus permettant de fixer le périmètre des usages sur lequel l'entreprise doit avoir le contrôle. A partir de là, elle doit pouvoir donner la possibilité aux collaborateurs eux-mêmes d'avoir cette compréhension de leurs usages, en leur fournissant les indicateurs sur la nature pro ou perso de ceux-ci. Cela facilitera d'autant la mise en conformité RGPD au global et leur acceptation de ses enjeux. De plus, il est prouvé que communiquer sur le sujet tend à responsabiliser les individus dans leurs pratiques.

" COMMENT FAIRE POUR QUE LE RGPD NE SOIT PAS UN FREIN AU BUSINESS ? "

A quel point les collaborateurs sont-ils sensibles au fait que leur entreprise s'intéresse ainsi à la répartition entre leurs usages personnels et professionnels ?

Quand les terminaux sont fournis par l'entreprise (COOP) – comme c'est le cas dans la majorité des entreprises d'une certaine taille en France – cela fait partie du « deal ». Mais l'entreprise doit surtout profiter de la meilleure compréhension qu'elle va avoir des usages en question pour clarifier ses engagements et ses attentes. De manière générale, vis-à-vis des collaborateurs, le RGPD est l'occasion de mettre tout le monde sur la même longueur d'onde. Un cadre légal va exister, et va pouvoir être prolongé par les entreprises par des chartes d'usage. Cela permet de déterminer qui est responsable de quoi et dans quelle circonstance. On sort alors du flou qui prévalait souvent, et les collaborateurs sont bien mieux intégrés dans la démarche du RGPD de façon transversale. Ce qui facilitera sans doute par extension leur engagement vis-à-vis des clients en la matière.

saaswedo

Cette enquête a été menée par Alliancy sur une idée propulsée par Saaswedo.
Rédaction des textes par Alliancy.

A propos de Saaswedo

Saaswedo est un éditeur de logiciels de gestion des actifs IT et Télécom qui fournit des solutions innovantes et performantes 100% SaaS. Depuis plus de 15 ans, Saaswedo délivre aux entreprises des offres qui permettent de maitriser leur politique IT et télécom, de simplifier la gestion de leurs actifs et d'optimiser leurs coûts. Saaswedo est éditeur de la solution Datalert, dédiée au contrôle des usages data mobile en temps réel.
Les solutions de Saaswedo ont été déployées dans plus de 80 pays, auprès de plus de 10 000 entreprises et gèrent 3.5 millions de lignes.
www.saaswedo.com

A propos d'Alliancy

Alliancy, numérique et business, et réciproquement...

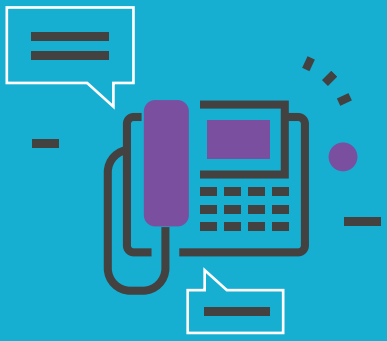
Stratégies, organisation et management, place de la data, nouveaux écosystèmes IOT, importance de la sécurité, gouvernance du SI... Alliancy est un magazine engagé en faveur du « travailler ensemble pour innover plus vite » et interroge les leviers de la transformation numérique pour qu'ils s'invitent peu à peu dans votre quotidien.
www.alliancy.fr

Saaswedo Headquarters
32 rue des Jeûneurs
75002 Paris – France

Saaswedo US
3423 Piedmont Rd NE
Atlanta, GA 30305

© 2018 Saaswedo. Tous droits réservés. Crédits photos : iStock. Conception : PourAction. Misterfish.

GUIDE PRATIQUE SAASWEDO



saaswedo en partenariat avec Alliancy